Oliver Leistert

Social Bots als algorithmische Piraten und als Boten einer techno-environmentalen Handlungskraft

2017

https://doi.org/10.25969/mediarep/2756

Veröffentlichungsversion / published version
Sammelbandbeitrag / collection article

Empfohlene Zitierung / Suggested Citation:
Leistert, Oliver: Social Bots als algorithmische Piraten und als Boten einer techno-environmentalen Handlungskraft. In: Robert Seyfert, Jonathan Roberge (Hg.): *Algorithmuskulturen. Über die rechnerische Konstruktion der Wirklichkeit.* Bielefeld: transcript 2017, S. 215–234. DOI: https://doi.org/10.25969/mediarep/2756.

9. Social Bots als algorithmische Piraten und als Boten einer techno-environmentalen Handlungskraft

Oliver Leistert

Wer sich dem komplexen Gegenstand der Social Bots unkritisch nähert, indem das *Social* darin affirmiert wird, handelt sich eine Reihe von Problemen ein, die aus den Umgebungen stammen, in denen zahlreiche dieser Bots heutzutage zu hause sind: denn der Begriff »Soziale Medien« selbst ist umstritten, wurde er doch vor allem mit einer kommerziellen, anstatt mit einer zunächst unkodierten, offenen Sozialität verschaltet. Grundsätzlich ließen sich Social Bots definieren als Entitäten, die »mit menschlichen Benutzern direkt mittels Sprache in zwei Richtungen kommunizieren« (Graeff 2014: 2), während sie dabei ›echte‹ Benutzer imitieren (Hingston 2012). Aber die Unterscheidung in ›echte‹ und ›nicht-so-echte‹ Benutzer erscheint dabei schon bald als eher naive Differenzierung, wenn in Anschlag gebracht wird, dass die ›echten‹ Benutzer von kommerziellen Plattformen sozialer Medien am Ende doch nur deren Kunden sind, z.B. Werbe- oder Überwachungsagenturen.

Das genannte Merkmal von natürlicher Sprachverarbeitung und -produktion jedoch, wenn auch weiterhin eher rudimentär, taugt zur Qualifizierung für Sozialität. Allerdings würde dies als Startpunkt einer Analyse von Social Bots diese unweigerlich primär ins Register von Signifikationsregimen einschreiben. Diese jedoch sind selbst durch Plattformen sozialer Medien bereits gekapert und überkodiert worden (Langlois et al. 2015).

Dieser Beitrag nimmt deshalb einen anderen Weg, und versucht Bots aus der Perspektive ihres Environments zu untersuchen, als Teil und Element einer medien-technischen Umgebung. Gleichzeitig ist es notwendig, Bots ins Verhältnis zur Logik des zeitgenössischen kapitalistischen Imperativs der Datenextraktion und dem Kolonisieren jeglicher, noch so unbedeutender Äußerungen von Benutzern auf den Plattformen zu setzen. Der Beitrag wird deshalb argumentieren, dass Bots auf kommerziellen Plattformen (1) als ›natürliche Bewohner‹ dieser Plattformen zu verstehen sind, die die Logik dieser

Plattformen und Protokolle selbst hervorbringt, und (2) dass zunehmend ein Symptom bedeutsam wird, dass ›algorithmische Entfremdung‹ genannt werden könnte. Dies ist ein Prozess, der gegenwärtig die gesamte Wissens- und allgemein Kommunikationsproduktion umbaut, wie vielfach in diesem Buch gezeigt wird.

Eine relationale Existenz eines digitalen Milieus, das durch Vertrauen gespeist wird

Anthropozentrische Theorien des Sozialen würden die Idee, dass Bots sozial sein können, wahrscheinlich ablehnen. Jenseits dieser Theorien hat sich jedoch eine Art Konsens eingestellt, der das Soziale nicht exklusiv dem Menschen (oder auch Tieren) zugesteht, sondern Akteursqualitäten zunächst allen Wesen und Dingen zuschreibt, da es am Ende Prozessketten unterschiedlichster Akteure und Aktanten sind, die Sozialität real werden lassen (Thrift 2005). Besonders Medien- und Technikwissenschaften fragen vermehrt nach dem ›wie‹ und ›wer mit wem‹, und weniger nach dem ›was‹ dieses Feldes. Damit zeigen sie an, dass es zur Analyse ihrer Gegenstände von Vorteil ist, anstatt weiterhin nach passenden Objekten für sterile Kategorien zu suchen, den Fokus stattdessen auf Fragen der Relation, Operationen und Performativität zu legen.

Ebenso ist das wechselseitige Bedingungsverhältnis von Technik und Gesellschaft ein Ausgangspunkt vieler Analysen geworden (Boczkowski 1999). Jüngere Beiträge der Science and Technology Studies, die explizit medienwissenschaftliche Ansätze integrieren, versuchen die Suche nach dem ›wer‹ oder ›was‹ hinter sich zu lassen (Gillespie et al. 2014), ähnlich wie Akteur-Netzwerk-Theorien, die auf Symmetrie in der Beschreibung von Technik und Gesellschaft abstellen, und den wechselseitigen Austausch sich gegenseitig anregender Aktanten in den Blick nehmen (vgl. Latour 1999). All dies hat zu einem Wechsel der Perspektiven geführt und einem Übergang von der Fixierung auf statische Wesen und Objekte hin zu Relationen und Dynamiken, die von allerlei Sorten von Aktanten und Akteuren in Bewegung gesetzt und ausgehandelt werden.

Dieser Perspektivwechsel ist auch für die Analyse von Bots hilfreich, denn was Bots zweifellos in erster Linie auszeichnet, ist ihr permanenter Versuch, mit anderen Akteuren Relationen aufzubauen, und weniger ihre ontologische Essenz oder ihr statisches Beharrungsvermögen. Dies trifft sowohl für die hochentwickelten Social Bot Netze auf Facebook zu, wie auch für die eher simplen Spambots, denn alle Bots versuchen sich über Datenaustausch mit Menschen zu verbinden, oder einen Datenaustausch, der Menschen indexiert, wie z.B. Kreditkartendaten, zu initiieren, oder einen Austausch anzubahnen,

indem Menschen z.B. über Phishing-Websites in Relation zu Bots gebracht werden.

In diesem Sinne sind Bots ein Spiegel unserer eigenen Eingeschlossenheit in Maschinen-zentrierten Milieus, die auf eine Amalgamierung von techno-kulturellen Gesellschaften mit Netzwerkinfrastrukturen hindeutet. Bots zeigen damit, dass die soziale Funktion *Vertrauen* in sozialen Medien algorithmischer Natur ist.[1] Vertrauen ist zu einer relationalen Sache von Verrechnung geworden, indexierbar und operationalisiert, um nur am Ende von Menschen angenommen oder abgelehnt zu werden. Vertrauen ist zu einem diskriminierbaren Parameter mutiert, der von Maschinen vorgeschlagen wird. Die algorithmische Produktion von Vertrauen, mit der Bots arbeiten, ist dabei tief eingebaut in die Logik der Ausbeutung und Wertextraktion kommerzieller Plattformen. Vertrauen in und durch algorithmische Operationen zeichnet somit ein neues Bild desselben, dass sich von jedem humanistischen Konzept von Vertrauen gelöst hat, und ausschließlich nach den Regeln von Berechenbarkeit arbeitet. Und dies ist eben dasselbe Milieu, das Bots bewohnen.

Das kommerzielle Zuhause von Social Bots

Um sich der Entwicklungslinie heutiger Social Bots anzunähern, sollen zunächst die Verschiebungen in Richtung eines algorithmischen Regimes von Medientechniken, das vom Motor der Monetarisierung und der kapitalistischen Einhegung angetrieben ist, gezeichnet werden. Die Ausweitung und explosionsartige Vermehrung der Social Bots in den letzten Jahren geht Hand in Hand mit dem gigantischen Erfolg kommerzieller Plattformen sozialer Medien, die seit einigen Jahren das soziale Gewebe dramatisch verändert und herausgefordert haben. Dies betrifft u.a. unser Verständnis von Öffentlichkeit (Baym und Boyd 2012), Freundschaft (Bucher 2013), kollektiven Protesten (Dencik und Leistert 2015), sowie allgemein großen Veränderungen innerhalb der Datensphären (Langlois et al. 2015).

Diese Entwicklungen sind mit einer starken Verschiebung von Datenschutzbestimmungen in Richtung privater Akteure einhergegangen (Braman 2006; Hintz 2015). Das Zusammenführen staatlicher und kommerzieller Überwachung (Landau 2010; Bauman und Lyon 2013) ist zu einem komplexen Konfliktfeld in der Beziehung zwischen Bürgern und ihren Regierungen (siehe www.dcssproject.net) durch den unaufhaltsamen Aufstieg der Daten-

1 | Es handelt sich hierbei jedoch nicht um das Vertrauen, das gemeint ist, wenn von Verschlüsselung gesprochen wird. Dies antwortet zwar auf ein ähnliches Problem – Vertrauen in vernetzten Umgebungen –, die Mittel dafür sind jedoch in den Händen der Benutzer, wenn es um Ende-zu-Ende Verschlüsselung geht.

imperien der sozialen Medien geworden. Seit den Enthüllungen von Edward Snowden (Greenwald 2014) ist bekannt, dass und wie diese Plattformen einen wesentlichen Anteil am Überwachungs-Gefüge (Haggerty und Ericson 2000) haben, das sich aus unzähligen heterogenen Datenbestände speist (Lyon 2014), um Erkenntnisse durch Mustererkennung und Korrelationen von Daten zu gewinnen.

Eines der Probleme, das durch diese neuen algorithmischen Regime aktuell geworden ist, sind die Auseinandersetzungen darüber, durch wen und wie die gesammelten Daten verwertet werden dürfen. Dies bleibt vorerst eine Konfliktlinie echtem globalen Ausmaßes, die sich durch zahllose politische und auch juristische Prozesse ausdrückt. Ein wichtiger Aspekt dabei bezieht sich auf die zunehmende Privatisierung von Kommunikation, bei der das alltägliche Gemurmel von Millionen von Menschen zum Eigentum der Plattformbetreiber mutiert. Dieser Aspekt ist als »digitale Einhegung« (Andrejevic 2007) bezeichnet worden, und meint die Übernahme (Einhegung) ursprünglich nicht-privatisierter Kommunikation für das Data Mining und den Datenverkauf an Dritte. Zusätzlich jedoch wirkt sich das so Eingehegte auf die Benutzer aus, da zum Mining und Verkauf der Daten dieselben notwendig streng präformatiert sein müssen: eine Präskription, die sich auf die Äußerungsbedingungen und das Sagbare überhaupt auswirkt. Diese Machtformation ist weich und verläuft gern unterhalb der Wahrnehmung. Dass Zensur hier meist nur durch die Nutzungsbedingungen geregelt wird, zeigt an, welche Macht über das Sagbare diese Konzerne in digitalen Kulturen gewonnen haben. Es ist dieses Auftauchen von globalen Datenbank-Imperien wie Facebook innerhalb weniger Jahre, das natürlicherweise alle möglichen Interessenten auf den Plan ruft, die ihren Anteil an den gespeicherten Daten fordern, auch jenseits von offiziellen Shareholdern, Überwachungsagenturen und Werbefirmen. Aus diesem Grund sind Social Bots nur als ein weiterer integrierter Interessent zu sehen, der sich in die Reihe derer einreiht, die Zugang zum verdateten Gewebe sozialer Relationen suchen und fordern. Dies erklärt u.a. warum Twitter zu einer wahren Botsphäre geworden ist. Im Jahre 2014 hat Twitter zugegeben, dass ungefähr 8,5 % aller Accounts auf Twitter Bots zuzuordnen sind. Dies entspricht rund 23 Millionen in absoluten Zahlen, auf die nochmals 5 % reine Spambots kommen (Goldman 2014).

Jenseits von legal und illegal: kommerzielle Plattformen bereiten den Bots ihren Weg

Um das massenhafte Erscheinen von Bots auf kommerziellen Plattformen wie Twitter oder Facebook zu untersuchen, sind die Rechtsdiskurse, die, wie Michel Foucault (2016) gezeigt hat, stets moralisch sind und auf Kontrolle abzie-

len, wenig zielführend, da Bots unter solchen Gesichtspunkten nur innerhalb eines bereits vordefinierten Spiels gefasst werden: als Eindringlinge gegenüber dem Regime, das den Raum, in dem sie auftreten, organisiert. Darum werden diese vernetzten Programme meist als Troublemaker innerhalb eines sonst sauberen, gepflegten privaten Datenbank-Imperiums diskutiert (vgl. Dunham und Melnick 2008), um sofort nach rechtlicher Regulierung zu rufen (Schellekens 2013), die unterscheiden soll zwischen legalen, regime-konformen und bösartigen, regime-devianten Bots. Letztere sind aber nichts weiter als die unbequeme Erinnerung daran, dass das Versprechen von Konzernen wie Facebook, eine sauber und sicher vernetzte Umgebung bereitzustellen, im Unterschied zum ›gefährlichen‹ offenen Internet, unmöglich einzuhalten ist, solange diese Konzerne selbst radikal neoliberale, von Kapitalinteressen geleitete Unternehmungen sind. Diese Plattformen, mit all ihren Mutationen und Aneignungen vernetzter Logiken, waren es selbst, die diesen räuberischen Feldzug kapitalintensiver Operationen zu einer neuen schizophrenen Intensität geführt haben, indem sie die Datenakkumulation und -verwertung mit einem Ambiente totaler Überwachung perfekt zusammengebracht haben. Hieran schließt die Produktion und das Betreiben von Social Bots nur an, und damit auch die Entstehung einer eigenständigen Bot-Ökonomie, die gegen Geld z.B. alle, die nach Aufmerksamkeit und Sichtbarkeit auf Twitter suchen, mit der exakt gewünschten Anzahl von Followern versorgt (Messias et al. 2013). Bots nutzen den Virus, den kommerzielle Plattformen erst in voller Blüte in heutige Subjektivitäten eingebracht haben: Sei sichtbar, vergleiche und ranke, sei wichtig, aber eben nur als eindeutig unterscheidbares und anschreibbares Individuum.

Im Kern nutzen Bots bei ihren Anbändelungen die harte Währung des Vertrauens aus, die grundlegend die sozialen Verhältnisse dieser Plattformen regelt. Darum ist es auch kaum erstaunlich, dass der Diskurs zu Social Bots oft bestimmt ist durch Fragen der Verschmutzung der öffentlichen Sphäre durch Bots, oder Problemen von Glaubwürdigkeit (Hingston 2012), sowie der ungenauen algorithmischen Beurteilung von Benutzern und ihrem Einfluss (Messias et al. 2013). Die Tatsache, dass inzwischen Forschungen angestellt werden, um diejenigen Benutzer zu identifizieren, die am anfälligsten für Bot-Anbändelungen sind (Wagner und Strohmeier 2010), indiziert dabei nur eine weitere Verschiebung vernetzter Verantwortung in kommerziellen Sphären, indem nun die Benutzer dieser Plattformen für ihr blindes Vertrauen gegenüber Bots verantwortlich gemacht werden. Dabei sind sie es ja erst, die mit unbezahlter Arbeit im Regime der geschlossenen Plattformen deren Wert erzeugen (Andrejevic 2011; Fuchs 2013).

Es ist dieser schizophrene Vorschub durch kommerzielle Plattformen, sich einerseits das Denken und die Affekte von Millionen Menschen anzueignen, während sie andererseits Felder des Begehrens produzieren, die dann den Rüs-

tungswettlauf zwischen Botprogrammierern anfeuern (Boshmef et al. 2011). Denn die Gegenmaßnahmen stammen aus demselben Arsenal wie die Bots selbst, so z.B. wenn dieselben algorithmische Verfahren angewandt werden, um Follower auf Twitter in echte und unechte zu unterscheiden (Bilton 2014), oder, im Falle Facebooks, das sogenannte ›Facebook Immune System‹ (Stein et al. 2011), das u.a. versucht, Bots zu identifizieren, um sie dann zu neutralisieren.

Darum ist der Versuch, zwischen guten und bösen Bots zu unterscheiden, unmittelbar verschränkt mit dem Problem von Besitz von und Zugang zu den Datensilos. Ob die Bots nun ›offiziell‹ sind oder Piraten, in jedem Fall sind sie herausragende Beispiele einer »fundamentalen Unsicherheit darüber, zu wem wir sprechen« (Gillespie 2014: 192) in Zeiten algorithmisch produzierter Öffentlichkeiten (Anderson 2012; Snake-Beings 2013).

Es ist dies darum ein massenhafter Fall für einen (umgedrehten) Turing-Test: im Feld der kritischen Internet-Forschung werden Bots als Spiegel unserer eigenen Reduktion auf Maschinen-ähnliche Akteure innerhalb dieser hochgradig standardisierten Umgebungen gesehen. »Social Bots sind die Reflektion unserer Aktivitäten auf sozialen Medien; damit diese Maschinen funktionieren, müssen wir selber zu einer Maschinenartigkeit trainiert werden« (Gehl 2014: 16). Dies bedeutet nichts anderes, als dass wir zu Produzenten von »aggregierten Mustern textuell formatierter, diskreter Geisteszustände« (34) geworden sind. Diskrete Zustände des Kognitiven sind genau die (Vor-)Bedingung für Komputation und ermöglichen das Bestehen des (umgedrehten) Turing Tests. Deshalb ist (ohne jeglichen Zynismus) festzustellen, dass die erfolgreiche Mobilisierung großer Teile der Bevölkerung, sich einem Turing Test zu unterwerfen, im Gegenzug die Bots als gleichberechtigte Partner qualifiziert.

Der unmögliche Katalog der Botsphäre

Es ist herausfordernd, wenn nicht sogar unmöglich, Bots zu typisieren, da es sich um ein hochdynamisches Feld handelt, das in großer Abhängigkeit zu den Plattformen und Umgebungen, auf denen die Bots laufen, steht. Dennoch folgt hier ein Versuch, anhand einiger Beispiele und Charakterisierungen die Bedeutung aber auch Diversität von Bots in heutigen Internetassemblagen darzustellen.

Dabei ist bereits die Formulierung, dass Bots auf Plattformen laufen, in vielen Fällen problematisch, da Bots auch dezentral auf externen Servern operieren können, die mit den Plattformen vernetzt sind, wie das Beispiel der Wikipedia-Bots zeigt (Geiger 2014). Auch ist dies ein weiterer Hinweis, dass Typisierungen den Relationen in diesem Feld epistemisch unterlegen sind. Des Weiteren hat die negative Bestimmung von einigen Bots (›malicious‹) dazu

geführt, sie identifizieren zu wollen, sie abzuschalten, oder auf andere Weise einzufangen (z.B. indem ihre Aktivität selbst nur auf Bots gerichtet wird, oder indem Anti-Bot Bots programmiert werden). Ein ganzer informatischer Forschungsstrang versucht Bots zu programmieren, die Bots eliminieren, was inzwischen zu einem intensiven Wettlauf zwischen Bot-Programmierern und Antibot-Bot-Programmierern geführt hat (Wang 2010). Solch Wettkämpfe induzieren jedoch weitere Komplexität ins Bot-Milieu, denn es wird immer schwieriger, Bots als klar umgrenzte Objekte zu erfassen. Bots können inzwischen höchst flexibel programmiert sein, ihr Verhalten ändern, und sogar (maschinen-)lernen (Boshmaf et al. 2012), was wiederum zu weiteren Anpassungstechniken führt. Die Bot-Milieus selbst machen die Situation noch komplizierter, durch ihre standardisierten Eingabemasken, dem Handling von Strings z.B. bei der Sentiment Analyse, und den Datenbank-basierten Berechnungen von Relationen. Je mehr die Internetkultur eine Template-Kultur mit standardisierten Schnittstellen geworden ist, umso einfacher ist die Simulation von Agilität und Lebhaftigkeit, da deren Ausdrucksweisen im Netz stark eingeschränkt und mutiert sind, um prozessierbar und korrelierbar zu sein. Mit Verweis auf Baudrillard ließe sich sagen, dass die Simulation eben ihre eigenen (Bot-)Kinder hervorbringt.

Auch die technische Beschreibung von Bots als halb- oder vollautomatische Agenten sagt wenig über die Rolle aus, die sie in verdateten kapitalistischen Umgebungen annehmen. Bots sind weit mehr als ihr Code (dies trifft auf jede Software zu). Ihre Eleganz und Handlungsfähigkeit wird erst relevant, wenn der Code in einer vernetzten Umgebung auch exekutiert wird. Man kann sich Geiger nur anschließen, der schreibt, dass »Bots deutlich daran erinnern, dass das, was Software ausmacht, nicht auf Code reduziert werden kann und nicht von den Bedingungen geschieden werden kann, unter denen sie entwickelt und deployed wird« (Geiger 2014, 246). Darum schlage ich weiter unten die Figur des algorithmischen Piraten vor, denn damit lassen sich Bots innerhalb einer politischen Ökonomie situieren, womit ein wichtiger neuer Layer in ihre Analyse eingezogen wird, der gleichzeitig eine metaphorische und somit *Bedeutung* produzierende Beschreibung für ansonsten asignifikante Maschinen erlaubt.

Zur Beschreibung und Unterscheidung von Bots schlage ich vorläufig nur zwei Kriterien vor: *Zweck (oder Absicht)* und *Software*. Zweck fragt nach dem Ziel der Programmierung und versucht eine Untersuchung ihrer Performance innerhalb und in Relation zum Bot-Milieu bereitzustellen. Software dient als Kurzform ihrer technischen Implementierung, die, würde sie umfassender ausfallen, notwendigerweise die Bibliotheken, technischen Standards, Netzwerkkapazitäten, Programmiersprachen und die Server, auf denen sie laufen, inklusive der Hardware, umfassen würde.

Jenseits dieser Elemente und Komponenten müsste eine auf Vollständigkeit zielende Beschreibung von Bot-Assemblagen sicherlich auch den Produktions- bzw. Programmierprozess, den Austausch unter den Programmierern, die Iterationen und Anpassungen der Bots im Betrieb, z.B. durch die Steuerung von Botnetzen, dazugehören. Auch muss die behauptete Automatisierung von Bots kritisch hinterfragt werden, da Updates oft manuell als Reaktion auf Veränderungen im Bot-Milieu erfolgen.

Beispiele von Bots, mehr oder weniger sozial

Als erster dieser halb- oder vollautomatischen, vernetzten Software-Agenten wären die *chatter bots* zu nennen, deren Zweck es ist, Aufgaben zu übernehmen, die für Menschen zu monoton sind, die aber erledigt werden müssen, um die Anwendung, in der sie aktiv sind, am Laufen zu halten. Vielleicht die ältesten Vertreter dieser Sorte sind Internet Relay Chat (IRC) Bots, »die in bestimmten Kanälen aktiv sind, deren Regeln und Gesetze anwenden, indem sie öffentliche Konversationen mitverfolgen, und aktiv werden gegen jene, die gegen die Regeln verstoßen, als auch manchen Benutzern auf Anfrage den Status eines Operators zuweisen« (Latzko-Toth 2014: 588). IRC-Bots werden, wie Latzko-Toth erläutert, auf die eigentliche IRC-Software obendrauf programmiert, die ihr Milieu darstellt, als zusätzlicher Code, um Management- und Systempflegeaufgaben auszuführen. Sie erledigen Steuerungsaufgaben, oder anders ausgedrückt, unterstützen das Regieren der IRC-Kanäle. Ihre Fähigkeiten variieren stark und sind ultimativ begrenzt durch die Möglichkeiten, die die IRC-Software selbst zulässt. Allerdings wurden in den Jahrzehnten der Benutzung von IRC unzählbare Patches und Erweiterungen programmiert, sodass Bots weit über den ursprünglichen Funktionsumfang dieser Open Source-Software hinaus Regulierungsaufgaben in diesem sozialen Medium *avant la lettre* umsetzen.

Ähnlich den IRC-Bots sind auch Bots auf Wikipedia kleine Helfer, die im Wesentlichen zwei Kernaufgaben ausführen. Erstens helfen sie mit, die riesige Wikipedia-Community mittels Steuerungsroutinen algorithmisch zu regieren. Mein Vorschlag ist deshalb, sie *governer bots* zu nennen. Ihr Zweck ist es »dass ein bestimmtes Maß an Uniformität in Stil und Inhalt gewährleistet wird«, und »sie dienen Schlüsselfunktionen der Kontrolle, indem sie besonders für Anfänger selbstständig diskursive und epistemologische Normen durchsetzen« (Geiger 2014, 345). Um ein Beispiel zu nennen: Zum Zeitpunkt dieser Niederschrift gibt es für die englischsprachige Wikipedia 1903 zugelassene Aufgaben für Bots (Wikipedia 2015a) und eine spezielle Wikipedia-Gruppe von Benutzern, die diese Armada von Bots überwacht und reguliert.

Zweitens schreiben einige Bots auf Wikipedia tatsächlich Artikel, oder Gerüste davon. So z.B. »der sogenannte Rambot, der von Ram-Man betrieben wurde, und ungefähr 30.000 Artikel über Städte in den USA, basierend auf Zahlen der US-Zensusbehörden, mit einer Rate von Tausenden am Tag schrieb« (Wikipedia 2015b). Allerdings ist zu bemerken, dass je nach Sprache, die Zahl dieser Bots auf Wikipedia stark variiert.[2]

Den Wikipedia-Bots, die Artikel schreiben, verwandt, sind Bots, die Rezensionen und Empfehlungen schreiben, besonders auf Shopping-Portalen oder allgemein Empfehlungsdiensten. Da das Ziel dieser Bots jedoch die Steigerung des Verkaufs von Produkten ist, indem sie eine ›authentische Erfahrung‹ mit dem Produkt simulieren, teilen diese Bots bereits einen Aspekt mit der Figur des Piraten, da sie versuchen Meinungen zu manipulieren, Wünsche zu produzieren, und ultimativ Geldflüsse anzuregen oder zu verändern. Allerdings ließe sich auch argumentieren, dass diese Zwecke sowieso ein inhärenter Teil der Marktlogik sind.

Aus diesem Grunde lässt sich der Empfehlungs-Bot sowohl als Schurke als auch als gutmeinender Ratgeber interpretieren, abhängig von seinem konkreten Milieu. Auf Amazon würden die meisten Benutzer solch einen Bot gewiss als hilfreich betrachten, oder ihn einfach ignorieren, während er auf diversen Preisvergleichsportalen eher als schurkenhaft einzustufen wäre, auf jeden Fall als illegitim. Jedoch sind die Kunden dieser Bots, die für ihre Entwicklung und ihren Einsatz bezahlt haben, letztlich selbst eng verzahnt mit Handelshäusern oder Werbeagenturen. Von daher sind Empfehlungs-Bots natürliche Erscheinungen einer datengetriebenen Ökonomie. Ihr Zweck ist die Verknüpfung von Waren-Daten und Geld-Daten. Die Verbindung zwischen diesen beiden Daten-Kategorien, die sie versuchen bei den Benutzern zu initiieren, ist dabei die *ultimative Verknüpfung*, die überhaupt erreicht werden kann, da damit ein Kauf produziert ist.

Der nächste Kandidat dieser kleinen Übersicht der Bot-Welten operiert ebenfalls in den Gefilden der Meinungsmache und -manipulation, jedoch ist der Zweck ein anderer. *Sockenpuppen-Bots* können in unterschiedlichsten Milieus auftauchen und agieren, von Twitter bis Reddit. Ihr Ziel ist es, Diskussionen und Debatten zu beeinflussen, was bis zur Zerstörung der Kommunikations-Sphäre führen kann. Der Begriff, mit dem diese Aktivität oft beschrieben wird, lautet *astro-turfing* (Leistert 2013). Die Mittel, die diese Bots zur Verfügung haben, unterscheiden sich erheblich und reichen vom Fluten von Kanälen mit immer gleichen Nachrichten, womit eine kontinuierliche Diskussion unmöglich gemacht und zerstört wird, bis zum zielgerichteten ›Befeuern‹ identifizierter Meinungsführer, mit dem Ziel, sie außer Kraft zu setzen. Diese

2 | Wikipedia und Bots bilden ein höchst komplexes Ökosystem, siehe z.B. Geiger (2014) und Niederer und van Dijck (2010).

Bots stellen eine attraktive Alternative zur Zensur dar, da sie viel Lärm in die Kommunikation induzieren, und somit z.B. politische Diskussionen unmöglich machen, aber die Kanäle als solche nicht in ihrer (technischen) Funktionalität beeinträchtigen oder ausschalten. Regierungsabteilungen, religiöse Gemeinschaften und Konzerne, sie alle benutzen diese Art von Bots – und nicht nur in Krisenzeiten. Zusammengefasst induzieren Sockenpuppen-Bots zerstörende Vektoren in die algorithmisch produzierten Öffentlichkeiten, was sie mit der psychologischen Kriegsführung (PsyOps) verwandt macht (Paganini 2013).

Weit bekannt und am häufigsten auf Twitter anzutreffen sind Bots, die Benutzern folgen (›followen‹), um deren Bekanntheit und Ruhm zu steigern. Auch wenn dies eine riskante Strategie ist, da Beobachter den plötzlichen Anstieg an Followern oft bemerken, wird sie breit in diversen Feldern angewandt. Politiker und Popstars sind noch die gewöhnlichsten Kunden dieser *fame enhancing bots*. Jedoch sind diese Bots auch zum Standardrepertoire von Marketing und Public Relations geworden, um die Popularität und Bekanntheit von Marken und Produkten zu steigern. Dabei nutzt diese Sorte Bots die Soziallogik aus, die die Plattformen selbst propagieren, nämlich der soziale Imperativ, dass jede Meinung und jedes Gefühl wichtig ist und algorithmisch verarbeitet gehört, was zur Verinnerlichung von einer Überbietungslogik bei den Benutzern führt: zu sein, heißt vor allem sichtbar zu sein (Milan 2015), was aber bedeutet: wer sein will, muss sichtbarer sein als die anderen. Und um genau dieses ›sichtbarer‹ kümmern sich diese Bots, die sich selbst sehr schnell replizieren können, um dieser Logik umso besser folgen zu können.

Harvesters schließlich gehören der Sorte Bots an, die als algorithmische Piraten im vollen Sinne bezeichnet werden können. Sie infiltrieren soziale Netzwerke und versuchen möglichst viele Benutzer auf Facebook zu ›frienden‹. Dabei ernten sie permanent Daten von und über die Nutzer und versuchen gleichzeitig, ihre wahre Natur zu verschleiern und unerkannt zu bleiben. Ihre Profile sind komplex und wirken ›echt‹, bis hin zu simulierten Aktivitätsphasen, die Rhythmen wie Tag und Nacht oder Werktagen und Wochenenden angepasst sind. Im Kern attackieren sie die ökonomische Logik der Plattformen selbst, da sie die Daten, die sie ernten, an ihre Betreiber (genannt ›herder‹) ausleiten, und damit jene Daten, die die Plattformen selbst an Dritte verkaufen, abgreifen: Daten von und über die Benutzer der Plattformen. Diese Sorte Bots ist getarnt und ihre Existenz hängt an der Effektivität ihrer Tarnung, da sie mit Menschen als Menschen interagieren, im Unterschied zu *fame enhancing bots*, die sich nur zu einer Liste von Followern addieren.

Ganz eindeutig mit bösen Absichten von ihren Betreibern programmiert sind Bots, die es darauf abgesehen haben, Schadcode in Applikationen einzuschleusen, z.B. indem sie Benutzer auf Phishing-Websites leiten. Das Milieu dieser Bots ist sehr flexibel. Diese bösartigen Bots können auf Dating-Plattformen bis hin zu Twitter auf Beute lauern. Ihre Aktivität ist zielgerichtet kurz:

hat ein Benutzer auf den schadhaften Link geklickt, ist ihre Aufgabe erfüllt. Nichtsdestotrotz müssen diese Bots zuerst mit den Benutzern ›anbändeln‹, um glaubwürdig zu wirken. Diese Bots sind ebenfalls den algorithmischen Piraten zuzuordnen, da sie im Prinzip vertrauenswürdige Umgebungen, wie z.B. Dating-Plattformen, ausnutzen, um den Datenverkehr aus ökonomischen Gründen in bereitgestellte Fallen zu lenken.

Social Bots als algorithmische Piraten des Datenkapitalismus

Aus der Perspektive einer politischen Ökonomie lassen sich, mit einigen Modifikationen, viele der vorgestellten Social Bots als wiedergekehrte Inkarnationen der Figur des Piraten beschreiben, weil sie zu dem gehören, was Lawrence Liang »ein ganzes Reich, das von Figuren wie Trickstern, Kopierern und Dieben bewohnt wird« (Liang 2010: 361) nennt. Social Bots als algorithmische Piraten zu modellieren, die, wie die Metaphorik bereitwillig hinzufügt, im Datenmeer der sozialen Medien schwimmen, ermöglicht einen Perspektivwechsel auf die Datenbankimperien kommerzieller sozialer Medien-Unternehmen, da die normalisierte Wahrnehmung und Auffassung über die Besitzverhältnisse von Daten dezentriert und somit erneut befragbar wird. Dies schließt einen neuen Blickwinkel für die Problematisierung der datenverarbeitenden Plattformen selbst mit ein. Social Bots, ob schurkenhaft oder nicht, ermöglichen somit eine erneute, veränderte Betrachtung heutiger Datenökonomien. Denn sie fragmentieren sowohl die in die Plattformen investierte unbezahlte affektive Arbeit heutiger post-fordistischer Subjektivitäten (Ross 2013), als auch das zeitgenössische Geschäftsmodell der Verwertung dieser Arbeit. Gleichzeitig sind sie am Ent- bzw. Wiederverwerten, indem sie die unbezahlte Arbeit und ihre Verwertung an einen »marginalen Platz der Produktion und Zirkulation« (Liang 2010: 361) lenken. Das Argument lautet deshalb, dass Social Bots die etablierten Kanäle und Schaltkreise unbezahlter Arbeit und ihrer Verwertung durch die Plattformen umformen, indem sie an diese Plattformen andocken: Sie erscheinen somit als das unterdrückte ›Andere‹, als jenes, welches in den zentralisiert regierten, vermauerten Reichen wie Facebook stets verdrängt, gelöscht, gesäubert werden soll, aber stets wiederkehrt und diese Reiche damit heimsucht wie ein unheimlicher Doppelgänger einer niemals ablegbaren, verdrängten Wirklichkeit.

Um jedoch die Operationalität dieser Social Bots aus einer solchen Perspektive genauer diskutieren zu können, ist ein kurzer Rekurs zum Diskurs der sogenannten Medienpiraterie notwendig, der erst die Reichweite und Limitierungen der Figur des algorithmischen Piraten klärt.

Medien und die Figur des Piraten

Sogenannte Medienpiraterie ist kein temporäres, sondern ein dauerhaftes Phänomen, und es ist weder neu, noch eine Anomalie kapitalistischer Unternehmungen. Lediglich durch den Übergang von Gutenbergs zu Turings Medienregime, sprich von Druckerzeugnissen zu digitalen Formaten, wurde das Thema in den letzten Dekaden prominent und umstritten diskutiert. Das alltägliche, massenhafte, halb- oder vollautomatische Kopieren und Verteilen von Software, Büchern, Musik und Filmen, on- und offline, hat enormen Druck auf die Copyright-Regime ausgeübt, die noch aus analogen Zeiten stammen, und somit aus einer teils vergangenen Phase kapitalistischer Akkumulation. Deren Konsolidierung und Institutionalisierung – in ihrer emblematischsten und zugleich symptomatischsten Form in der Gründung der Weltorganisation für geistiges Eigentum (WIPO) im Jahre 1970 – verläuft parallel zu zwei historisch herausragenden Phasen: zum offiziellen Ende der Kolonialzeit als politisches Regime, was zur Entstehung diverser neuer Nationalstaaten geführt hat, die begannen ihre eigene Agenda zu verfolgen, sowie zur vernetzten Vereinheitlichung von Märkten zu einem ›Weltmarkt‹, der von der USA, Westeuropa und Japan formiert und geführt wird. Hegemonieansprüche und -durchsetzungen im Bereich des sogenannten ›geistigen Eigentums‹ sind seitdem zu Machtformation geronnen, die die ›entwickelten‹ Staaten anderen aufzwingen.

Noch im 19. Jahrhundert jedoch waren die Verhältnisse anderes verteilt, da damals die USA mit der industriellen Entwicklung in Europa noch nicht gleichgezogen hatten. Um diese Ziel zu erreichen, war es eine gewöhnliche Praxis der US-amerikanischen Industrie, europäische Patente und andere Copyright-Ansprüche zu kopieren, und damit zu verletzen (Ben-Atar 2004). Heute sind es vor allem die USA, die versuchen sich gegen Staaten zu schützen, die ihrerseits mit solchen Verletzungen arbeiten, um ihre Industrie auf Weltstandard zu bringen, z.B. China oder Indien. Dies zeigt, wie natürlich der Prozess der Piraterie historisch in den kapitalistischen Entwicklungen zu sehen ist, da jede »Analyse von Piraterie die Grenzlinien und (Il)legitimitäten eines bestimmten Machtregimes anzeigt« (Zehle and Rossiter 2014: 345).

Die fortbestehende Dringlichkeit, Lösungen zu finden, die den Zugang zu Information und Wissen regeln, drückt sich durch die vielen sehr lebendigen Debatten zu den Gemeingütern (Commons) aus (Linebaugh 2013), sowie der wachsenden Zahl alternativer Copyright Regime, wie die Creative Commons (Lessig 2002), oder die viralen Software Lizenzen, wie z.B. die GNU-Lizenzen. Es geht dabei weiterhin darum, eine Balance zu finden zwischen dem Recht auf Zugang zu Information und Wissen, und den Interessen der inzwischen nicht mehr allmächtigen Urheberrechtsverwaltungen, wie der

RIAA[3]. Die vielen Versuche einer technischen Lösung für ein Problem, das letztlich ein Problem sozialer Gerechtigkeit ist, wie die Digitale Rechteverwaltung (DRM), erinnern daran, dass digitale Kulturen unter anderen Prämissen laufen, als vergangene Regime. Wenn es stimmt, dass »die Macht der Algorithmen von zunehmender Bedeutung der digitalen Rechteverwaltung für Medienkonzerne ist« (Lash 2007: 71), dann kommt innerhalb digitaler Milieus ohne Zweifel einer Reihe neuer Akteure und Aktanten Handlungsmacht zu.

Um Ansprüche auf geistiges Eigentum durchzusetzen, wurde ein mächtiger und angsteinflößender Diskurs zur Piraterie etabliert, in dem Piraten dargestellt werden »als die ultimative Verkörperung des Bösen. Dieses Böse kann eine Reihe von Formen annehmen, vom Terrorismus und des kriminellen Untergrunds, bis zum Verursacher des Untergangs der Unterhaltungsindustrie sowie von Steuerflucht« (Liang 2010, 356). Interessanterweise aber gilt zugleich für diejenigen Akteure, »die versuchen, das Anwachsen von Regimen geistigen Eigentums zu verhindern, und die öffentliche Domäne zu verteidigen, dass sie die Figur des Piraten peinlich berührt ignorieren oder direkt ablehnen« (Liang 2010: 356). Piraterie, so scheint es, ist bestimmt von einer Logik, die die wohl geordneten westlichen Konzepte von Eigentum und Legalität transversal durchkreuzt, wie ein Trickster. Piraten werden aus diesem Grund auch niemals ehrliche Verbündete der Anhänger von Gemeingütern sein können. Darüber hinaus wird Piraterie als Gefahr für die sogenannte Kreative Klasse verstanden, also letztlich als Feind der Künstler, deren legitime Interessen von den Piraten ignoriert werden. Dieser vermeidlich parasitäre Charakter von Piraterie verkennt jedoch dessen produktive Seite: Piraterie hat über unterschiedliche Märkte verteilt höchst kreative Formen der Distribution erfunden (Maigret/Roszkowska 2015). Und dies ist die entscheidende Parallele, die diese Piraterie mit der Art verbindet, wie piraterische Social-Bots-Daten weiterverteilen. Der Unterschied jedoch ist der Modus der Distribution. Daten, die Bots gesammelt haben, können in höchst unterschiedliche Richtungen verteilt werden, vom Kreditkartenbetrug bis zum Hacken von Websites, von erstaunlich passenden Werbeeinblendungen oder Spam bis zu Identitätsdiebstahl. Jedoch, egal welchen Modus der Redistribution die Daten nehmen und wie sie wieder eingesetzt werden, grundsätzlich sind sie für interessierte Käufer jeglicher Couleur verfügbar, exakt wie die sogenannten ›Medien der Piraten‹.

3 | Die Recording Industry Association of America (RIAA) ist nur eine von vielen Organisationen, die über die Einhaltung von Copyrightregimen wacht und mit äußerst dubiosen Mitteln versucht, diese auch durchzusetzen.

Piratenbots, Algorithmen und Infrastruktur

Die Macht der Piratenbots resultiert besonders aus der Macht der Infrastrukturen, die sie bewohnen. Es ist diese Verteilung von Machtrelationen innerhalb von Infrastrukturen, in denen sich die Modulation von Kontrolle – berühmt durch Gilles Deleuzes ›Postskript über die Kontrollgesellschaften‹ (1994) – materialisiert, und zwar als verteilte und dezentrale logistische Knoten. In den Senken dieser environmentalen Wirkmächigkeit artikulieren und replizieren sich die Piratenbots, denn »Piraterie suggeriert nicht nur einen dauerhaften Verlust von Räumen und Märkten, sondern auch ein Verbreitungsmodell, bei dem die ›Distribution‹ selbst zu einer produktiven Form wurde. Als Distributoren vervielfältigen Piraten Medien; Piraterie schafft mehr Piraterie« (Sundaram 2009: 116). Seit Algorithmen vermehrt Regulierungstätigkeiten übernommen haben (Ziewietz 2015) und als Analyseinstrumente breit eingesetzt werden (Amoore/Piotukh 2015), konnten Piratenbots Knotenpunkte oder Elemente einer Assemblage werden, die infrastrukturelle Operationen regelt. Piraterie nistet sich ein in dem, was Keller Easterling ›extrastatecraft‹ nennt (2014), um die physischen und nicht-physischen Machtformationen zeitgenössischer, globaler Infrastrukturökonomien zu beschreiben, die »den imperialen Anspruch auf Standards und Infrastrukturen« darstellen (Zehle/Rossiter 2014: 349). Genau dies ist aber auch das Milieu, in dem

> »Piraterie in warenförmigen Tauschkreisen existiert, nur dass hier das Selbe ins Viele sich verteilt. Verteilung in Form von viralen Schwärmen ist die Basis piraterischer Verbreitung, ihr Verschwinden in die versteckten Orte der Zirkulation ist das Geheimnis ihres Erfolges, sowie die Verteilung der Profite in diverse Stellen des Netzwerks.« (Sundaram 2009: 137)

Ebenso proliferieren Piratenbots, indem sie zu Schwärmen werden und wieder verschwinden.

In diesem Sinne ist Piraterie vielmehr als komplementär denn als parasitär zu verstehen, in einem Modus der »Relation, der die Resilienz (und Redundanz) von Netzwerkinfrastrukturen anzeigt« (Zehle/Rossiter 2014: 348). Konzerne wie Microsoft nutzten die Piraterie ihrer Produkte strategisch, um Konkurrenzprogramme aus dem Open Source Feld zu bekämpfen, die in der Regel kostenlos zu haben sind. Auch dies deutet auf eine analytische Qualität des Begriffs der Piraterie hin.

Insofern ist es durchaus möglich, Social Bots jenseits moralischer oder legalistischer Überlegungen in einer der Datenakkumulation verschriebenen kapitalistischen Ökonomie, die selber die Privatsphäre und informatische Selbstbestimmung strukturell angreift, zu situieren. Denn die heutige Internetökonomie wird im Wesentlichen von Datenmaklern und Unternehmen für

Werbung und Öffentlichkeitsarbeit angetrieben. Sie implementieren erfolgreich die Logik des Kostenlosen (»free as in free beer«), bei der die Monetarisierung auf undurchsichtigen Geschäften mit Daten beruht, von denen diejenigen, die die Daten liefern – die Benutzer – nichts mitbekommen. Social Bots sind insofern nur die unterdrückte, komplementäre Seite dieses Geschäftsmodells. Und während Medienpiraterie bereits seit Jahrzehnten ein vielschichtiger Kampfschauplatz ist, zeichnet sich ab, dass Datenpiraterie die nächste Stufe dieses Kampfes einer Ökonomie ist, die von Verdatung lebt. Indem sie erfolgreich die Währung ›Vertrauen‹ auf Sozialen Medien attackieren und ausnutzen, zeigen sie gleichzeitig den hohen Grad an *algorithmischer Entfremdung* an, den diese Plattformen produzieren. Die Tatsache, dass diese Bots es schaffen, erfolgreich als Menschen durchzugehen, bezeugt den äußerst prekären und sich wandelnden Status von Sozialität, der durch diese Plattformen Realität geworden ist.

Es ist in diesem Sinne interessant, dass diese dunkle Seite der Internetkultur bisher wenig erforscht wird. Jenseits der üblichen Ausnahmen (Parikka 2007; Parikka/Sampson 2009; Brunton 2013) scheint die Internetforschung selbst von den Mythen der Effektivität und Immaterialität des Netzes geblendet zu sein, der den Diskurs über das Netz seit den 1990ern formiert hat. Ein materialistischer Zugang müsste zu eben diesen vernachlässigten Figuren wie den Bots als algorithmische Piraten arbeiten, oder, um ein anderes Beispiel das kaum erforscht wird zu nennen, zu der Tatsache, dass die Pornoindustrie mittlerweile eine Schlüsselfigur in der Entwicklung von Standards wie Streaming-Technologien und Traffic Routing (Chun 2005) geworden ist. Das Internet als gigantische Maschine »um mehr Lärm zu produzieren« (Lovink 2005: 10), hat unzählige Aktanten. Social Bots gehören unbedingt dazu.

Des Weiteren können moralische oder legalistische Diskurse keine Erkenntnisse zur materiellen Seite des Internet produzieren: Facebooks Verbot der Darstellung stillender Mütter, bzw. deren Zensursystem generell, auch und gerade weil es legal ist, da es mit den Benutzungsbedingungen übereinstimmt, wäre ein weiterer Aspekt, der zeigt, dass Algorithmen Mitregierende in der Formatierung und Bewertung von Ausdrucksvermögen geworden sind. Sie bestimmen, was im kommerziellen Netz möglich ist und was nicht, und kontrollieren effektiv die Bedeutung von Beiträgen durch ihre vollkommen beschränkten und normativen Konzepte dessen, was Wörter und Bilder bedeuten – der Alptraum des Dichters.

Social Bots lassen sich insofern auch als Varianten solch Mitregierender verstehen, auch wenn sie teils inoffiziell oder schadhaft sind, und damit mit geringerer systemischer Handlungsfähigkeit als ihre ›Kollegen‹ ausgestattet sind, den offiziellen Algorithmen der Plattformen, mit denen sie konkurrieren. Darum ist die Sicht auf sie als Parasiten nicht ausreichend. Sie sind vielmehr das Komplementäre der Datenindustrie, möglich geworden durch die

Geschäftsmodelle selbst. Das Vertrauen, das sie angeblich missbrauchen, ist selbst hochgradig streitbar, da Einsicht in die Berechnungsprozesse, die es erzeugen, den Benutzern ebenfalls versagt bleibt. Indem solch elementare menschliche Bedürfnisse und Bedingungen wie Vertrauen an ›Maschinenintelligenz‹ delegiert wird, ist es unausweichlich, dass diese Maschinenlogik selbst ihr Anderes in Form von Bots als Möglichkeit produziert. Bots folgen damit lediglich dem Trend, den kommerzielle Plattformen zur Perfektion treiben, indem sie die Unterscheidung von Privat und Öffentlich kassiert haben.

Schließlich gilt, dass »algorithmische Technologien dazu neigen, Unterschiede der Art in Unterschiede des Grades zu verwandeln [...] oder zur Distanz eines Datenpunktes zu einem anderen« (Amoore/Piotukh 2015: 361). Solch eine flache Sozialität, die sich nur noch gradweise differenziert, wird aufgrund ihrer unbegrenzten Vermögen der Reproduktion und Distribution unumgänglich nur viel mehr Desselben produzieren können. Indem Bots dynamisch ihre simulierten Referenzen wechseln, und nach ihrer Neutralisierung wie eine Hydra in automatisch generierten Profilen wieder erscheinen, sind Social Bots als erste ›Natives‹ heutiger Umgebungen sozialer Medien zu verstehen, die sich selbst anhand ihrer einprogrammierten Reproduktionsregeln generisch reproduzieren können. Sie zu bannen und einzugrenzen wird auf lange Sicht wenig Erfolg haben, da die Plattformen selbst die menschlichen Subjektivitäten produzieren, die jene Kompatibilität aufweisen, die die Bots brauchen, um mit ihnen in Kontakt treten zu können. Wer sich von den Standardisierungen, Zensursystemen, Nutzungsbedingungen, Templates, algorithmischen Prozessen und Datenbank-basierten Vernetzungen regieren lässt, hat sich in der Logik der Kontrolle durch Protokolle (Galloway 2004) eingerichtet. Algorithmische Piraten, wie einige Social Bots es sind, haben keine Probleme, die Anforderungen dieser protokologischen Bedingungen zu bedienen und sind deshalb natürlicherweise prädestiniert dazu, aktive Rollen in solch einer environmentalen Logik der Kontrolle zu bekleiden.

Übersetzt von Moritz Plewa.

Literaturverzeichnis

Amoore, L./Piotukh, V. (2015): »Life beyond Big Data: Governing with Little Analytics«, *Economy and Society* 44 (3): S. 341-366.

Anderson, C.W. (2012): »Towards a Sociology of Computational and Algorithmic Journalism«, *New Media & Society* 15 (7), S. 1005-1021.

Andrejevic, M. (2007): »Surveillance in the Digital Enclosure«, *The Communication Review* 10 (4), S. 295-317.

Andrejevic, M. (2011): »The Work That Affective Economics Does«, *Cultural Studies* 25 (4-5), S. 604-620.

Bauman, Z./Lyon, D. (2013): *Liquid Surveillance a Conversation*, Cambridge, UK und Malden, MA: Polity Press.

Baym, N.K./Boyd, D. (2012): »Socially Mediated Publicness: An Introduction«, *Journal of Broadcasting & Electronic Media* 56 (3), S. 320-329.

Ben-Atar, D.S. (2004): *Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power*, New Haven, CT: Yale University Press.

Bilton, N. (2014): »Social Media Bots Offer Phony Friends and Real Profit«, *The New York Times*, 19. November, abgerufen auf: www.nytimes.com/2014/11/20/fashion/social-media-bots-offer-phony-friends-and-real-profit.html?_r=0 (zuletzt am 24. Oktober 2015).

Boczkowski, P. (1999): »Mutual Shaping of Users and Technologies in a National Virtual Community«, *Journal of Communication* 49 (2), S. 86-108.

Boshmaf, Y./Muslukhov, I./Beznosov, K./Ripeanu, M. (2011): »The Socialbot Network: When Bots Socialize for Fame and Money«, *Proceedings of the 27th Annual Computer Security Applications Conference*, ACM, S. 93-102, abgerufen auf: http://dl.acm.org/citation.cfm?id=2076746 (zuletzt am 16. Februar 2015).

Boshmaf, Y./Muslukhov, I./Beznosov, K./Ripeanu, M. (2012): »Key Challenges in Defending against Malicious Socialbots«, *Proceedings of the 5th USENIX Conference on Large-Scale Exploits and Emergent Threats*, USENIX Association, S. 12-12, abgerufen auf: www.usenix.org/system/files/conference/leet12/leet12-final10.pdf (zuletzt am 24. September 2015).

Braman, S. (2006): *Change of State: Information, Policy, and Power*. Cambridge, MA: The MIT Press.

Brunton, F. (2013): *Spam: A Shadow History of the Internet*. Cambridge, MA: The MIT Press.

Bucher, T. (2013): »The Friendship Assemblage: Investigating Programmed Sociality on Facebook«, *Television & New Media* 14 (6), S. 479-493.

Chun, W.H.K. (2005): *Control and Freedom: Power and Paranoia in the Age of Fiber Optics*. Cambridge, MA: The MIT Press.

Deleuze, G. (1993): »Postskriptum über die Kontrollgesellschaften«, ders. *Unterhandlungen 1972-1990*, Frankfurt a.M.: Suhrkamp, S. 254-262.

Dencik, L./Leistert, O. (Hg.) (2015): *Critical Perspectives on Social Media and Protest: Between Control and Emancipation*, London: Rowman & Littlefield.

Dunham, K./Melnick, J. (2008): *Malicious Bots: An Inside Look into the Cyber-criminal Underground of the Internet*, Boca Raton, FL, London und New York: CRC Press.

Easterling, K. (2014): *Extrastatecraft: The Power of Infrastructure Space*. London und New York: Verso.

Foucault, M. (2015): *Die Strafgesellschaft: Vorlesung am Collège de France 1972 – 1973*, Berlin: Suhrkamp.

Fuchs, C. (2013): »Class and Exploitation in the Internet«, Trebor Scholz (Hg.) *Digital Labor: The Internet as Playground and Factory*, New York: Routledge, S. 211-223.

Galloway, A. (2004): *Protocol: How Control Exists after Decentralization*, Cambridge, MA: The MIT Press.

Gehl, R.W. (2014): *Reverse Engineering Social Media: Software, Culture, and Political Economy in New Media Capitalism*, Philadelphia, PA: Temple University Press.

Geiger, R.S. (2014): »Bots, Bespoke, Code and the Materiality of Software Platforms«, *Information, Communication & Society* 17 (3): S. 342-356.

Gillespie, T. (2014): »The Relevance of Algorithms«, hg. v. T. Gillespie, P. J. Boczkowski und K. A. Foot (Hg.) *Media Technologies: Essays on Communication, Materiality, and Society*, Cambridge, MA: The MIT Press, S. 167-193.

Gillespie, T.,/Boczkowski, P.J./Foot, K.A. (2014): *Media Technologies: Essays on Communication, Materiality, and Society*. Cambridge, MA: The MIT Press.

Goldman, D. (2014): »23 Million Twitter Users Are Fed by Robots«, *CNN Money*, abgerufen auf: http://money.cnn.com/2014/08/12/technology/social/twitter-bots/index. html (zuletzt 1. November 2015).

Graeff, E.C. (2014): »What We Should Do Before the Social Bots Take Over: Online Privacy Protection and the Political Economy of Our Near Future«, Massachusetts Institute of Technology, Cambridge, MA, abgerufen auf: http://web.mit.edu/sts/Graeff.pdf (zuletzt am 7. Oktober 2015).

Greenwald, G. (2014): *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. London: Penguin Books.

Haggerty, K.D./Ericson, R. (2000): »The Surveillant Assemblage«, *British Journal of Sociology*, 51 (4): S. 605-622.

Hingston, P. (2012): *Believable Bots*, Berlin und Heidelberg: Springer.

Hintz, A. (2015): »Social Media Censorship, Privatized Regulation and New Restrictions to Protest and Dissent«, L. Dencik und O. Leistert (Hg.) *Critical Perspectives on Social Media and Protest: Between Control and Emancipation*, London: Rowman & Littlefield, S. 109-126.

Landau, S. (2010): *Surveillance or Security?: The Risks Posed by New Wiretapping Technologies*, Cambridge, MA: The MIT Press.

Langlois, G.,/Redden, J./Elmer, G. (2015): *Compromised Data: From Social Media to Big Data*. New York und London: Bloomsbury.

Lash, S. (2007): »Power after Hegemony: Cultural Studies in Mutation?«, *Theory, Culture & Society*, 24 (3): S. 55-78.

Latour, B. (1999): *Pandora's Hope: Essays on the Reality of Science Studies*, Cambridge, MA: Harvard University Press.

Latzko-Toth, G. (2014): »Users as Co-Designers of Software-Based Media: The Co-Construction of Internet Relay Chat«, *Canadian Journal of Communication* 39 (4), S. 577-595.

Leistert, O. (2013): »Smell the Fish: Digital Disneyland and the Right to Oblivion«, *First Monday* 18 (3), doi: 10.5210/fm.v18i3.4619.

Lessig, L. (2002): *The Future of Ideas: The Fate of the Commons in a Connected World*, New York: Vintage.

Liang, L. (2010): »Beyond Representation: The Figure of the Pirate«, A. Kapczynski und G. Krikorian (Hg.), *Access to Knowledge in the Age of Intellectual Property*, New York: Zone Books, S. 353-376.

Linebaugh, P. (2013): *Stop: The Commons, Enclosures, and Resistance*, Oakland, CA: PM Press.

Lovink, G. (2005): *The Principle of Notworking: Concepts in Critical Internet Culture*, Amsterdam: Amsterdam University Press.

Lyon, D. (2014): »Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique«, *Big Data & Society* 1 (2), doi: 10.1177/2053951714541861.

Maigret, N./Roszkowska, M. (2015): The Pirate Book. Ljubljana: Aksioma-Institute for Contemporary Art, abgerufen unter: http://thepiratebook.net.

Messias, J.,/Schmidt, L./Oliveira, R./Benevenuto, F. (2013): »You Followed My Bot! Transforming Robots into Influential Users in Twitter«, *First Monday*, 18 (7).

Milan, S. (2015): »Mobilizing in Times of Social Media: From a Politics of Identity to a Politics of Visibility«, L. Dencik und O. Leistert (Hg.), *Critical Perspectives on Social Media and Protest: Between Control and Emancipation*,London: Rowman & Littlefield, S. 53-70.

Niederer, S./van Dijck, J. (2010): »Wisdom of the Crowd or Technicity of Content? Wikipedia as a Sociotechnical System«, *New Media & Society* 12 (8): S. 1368-1387.

Paganini, P. (2013): *PsyOps and Socialbots: InfoSec Resources*, abgerufen auf: http://resources.infosecinstitute.com/psyops-and-socialbots/ (zuletzt am 29. Oktober 2015).

Parikka, J. (2007): *Digital Contagions: A Media Archaeology of Computer Viruses*. New York: Peter Lang.

Parikka, J./Sampson, T.D. (2009): *The Spam Book: On Viruses, Porn, and Other Anomalies from the Dark Side of Digital Culture*, New York: Hampton Press.

Ross, A. (2013): »In Search of the Lost Paycheck«, Trebor Scholz (Hg.), *Digital Labor: The Internet as Playground and Factory*, ew York: Routledge, S 13-32.

Schellekens, M.H.M. (2013): »Are Internet Robots Adequately Regulated?«, *Computer Law & Security Review* 29 (6): S. 666-675.

Snake-Beings, E. (2013): »From Ideology to Algorithm: The Opaque Politics of the Internet«, *Transformations: Journal of Media and Culture* 23, abgerufen

auf: www.transformationsjournal.org/issues/23/article_03.shtml (zuletzt am 28. Mai 2016).

Stein, T./Chen, E./Mangla, K. (2011): »Facebook Immune System«, *SNS 2011 Proceedings of the 4th Workshop on Social Network Systems*, ACM, S. 1-8.

Sundaram, R. (2009): *Pirate Modernity: Delhi's Media Urbanism*, London und New York: Routledge.

Thrift, N.J. (2005): *Knowing Capitalism*. London: Sage.

Wagner, C./Strohmaier, M. (2010): »The Wisdom in Tweetonomies: Acquiring Latent Conceptual Structures from Social Awareness Streams«, *SEMSEARCH '10 Proceedings of the 3rd International Semantic Search Workshop*, ACM, 6, abgerufen auf: http://dl.acm.org/citation.cfm?id=1863885 (zuletzt am 28. November 2014).

Wang, A.H. (2010): »Detecting Spam Bots in Online Social Networking Sites: A Machine Learning Approach«, *Data and Applications Security and Privacy XXIV*, Springer, S. 335-342.

Wikipedia (2015a), »Bots«, https://en.wikipedia.org/wiki/Wikipedia:Bots (zuletzt aufgerufen am 25. Oktober 2015).

Wikipedia (2015b): »History of Wikipedia Bots« https://en.wikipedia.org/wiki/Wikipedia:

History_of_Wikipedia_bots (zuletzt aufgerufen am 25. Oktober 2015).

Zehle, S./Rossiter, N. (2014): »Privacy Is Theft: On Anonymous Experiences, lnfrastructural Politics and Accidental Encounters«, J. Arvanitakis und M. Fredriksson (Hg.), *Piracy: Leakages from Modernity*, acramento, CA: Litwin Books, S. 345-353.

Ziewitz, M. (2015): »Governing Algorithms: Myth, Mess, and Methods«, *Science, Technology & Human Values*, online zuerst am 30. September.